Cyber Security Comments Template

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
1	6	2.2e. Fraud Prevention and Revenue Assurance – The NPSBN should have Fraud Prevention and Revenue Assurance functionality to ensure that resources are being used appropriately and charging and service control transactions are providing a true picture of network usage.	The State of Florida agrees that the NPSBN should have a fraud protection functionality to ensure those that are authorized to utilize the network and the Priority and Preemption Quality of Service receive these functionalities without interference from unauthorized users. The State, however, points out that many potential NPSBN users currently maintain an "unlimited data plan", which FirstNet should consider in order to promote user adoption. Additionally, the State believes it is imperative that charging and service controls are used to ensure end-to-end QoS for Public Safety rather than as a mechanism to attempt to reduce the data rate of Public Safety in order to "appropriately" monetize the excess capacity being used by secondary users.		
2	6	2.2j. Heterogeneous Networks – The NPSBN Cyber Security Solution should enable small cells and heterogeneous networks, potentially offered by a third party, to securely authenticate to and interconnect to the core network.	The State of Florida agrees that the network should enable small cells and heterogeneous networks to securely authenticate to and interconnect to the core network. Such a situation will allow for greater coverage indoors, for example, or reduce NPSBN congestion through WiFi-off-loading. The State comments that any "third party" hardware and software must be tested to ensure confidentiality, integrity, and availability. The State also notes that if Public Safety users are off-loaded to WiFi networks, the Offeror must maintain the same data confidentiality, integrity, and availability through appropriate protections. Additionally, if Public Safety users are off-loaded to WiFi, such data transmissions should not be billed in the same		

			manner as those transmissions utilizing the NPSBN resources.		
3	8	2.2v. Training – It is critical that human factors within cyber security be considered as one of the most important but most difficult areas to assess and protect. Training of users and operators should be one of the key methods to increase the cyber security of the NPSBN.	The State of Florida agrees that training the potential Public Safety users will be one of the most important factors in maintaining the security of data. The State believes that the Offeror will either directly, or via government subsidies, train all Public Safety users of the network. Additionally, the training should be consistent across the Nation, and provided on a continuous basis. Benchmarks will also help establish effectiveness of training materials (ex: a Phishing test to trainees).		
4	8	2.2. 3.a.v. Devices should be continuously monitored both "online" and "offline" to ensure the OS is not compromised and that devices have not been Jail Broken or Rooted.	The State of Florida requests a definition of "offline".		
5	9	2.2 3.g. Bring Your Own Stuff – Cyber security solutions should address "Bring Your Own (Device, Application, or Wearable)."	The State of Florida agrees that the Offeror's cyber security solution should address "Bring Your Own Stuff" as there are many smaller and voluntary agencies operating across the State that do not have the resources to purchase "agency-owned devices". The State maintains that the Offeror should work with individual agencies on policies regarding the data on the "stuff" (such as the need to wipe all organizational and personal data from a lost/stolen personal device being used for Public Safety operations).		
6	10	2.2 4.e. Application Security Certification –The solution should ensure all Mobile, Web, and Desktop applications operating on the NPBSN undergo a defined certification process to ensure usability, reliability, privacy, security, and safety.	The State of Florida agrees that all applications operating on the network undergo a defined certification process. The State believes this should go one step further to include minimum standards to be applied.		
7	11	2.2 4.l. Data Loss Prevention – The solution should provide protections to ensure applications protect data while at rest, in use, and in transit.	The State of Florida agrees that the solution should provide protections. This section is labeled as "Data Loss Prevention", but does not address prevention, rather this section solely focuses on		

			protection. The State believes that FirstNet should revise this section to include language related to prevention activities, while maintaining the protection clause.		
8	11	2.2. 5.b.i. Identity Assurance – The solution should ensure the following relationships are always authenticated:	The State of Florida agrees that authentication will be required to maintain cyber security. The State requests that FirstNet include a suggestion that relates to identifying each user when multiple users are sharing a single device simultaneously. For example, a shared mobile terminal in a Fire Engine, or multiple firefighters on a single mobile data computer.		
9	12	2.3 5.b-d. b. Risks that have no direct correlation to an internally controlled mechanism will be either accepted or transferred (e.g., through procurement of insurance against the risk). c. Those risks tied to a particular vulnerability or threat will be evaluated based on impact and viability of mitigation. d. Upon final ranking and evaluation, appropriate controls will be addressed.	The State of Florida requests further clarification on risk acceptance and viability of mitigation. The State believes it is imperative for FirstNet to weigh Public Safety risk at an appropriate level agreed upon in the State Plan. The State also requests clarification as to who shall be responsible for evaluating and ranking identified risks, as well as devising and implementing subsequent controls. The State would also request clarification as to who will be responsible for procuring the referenced insurance against risk and what the mandated insurance limits will need to be.		
10	13	2.4 1.e. Communicate among internal and external stakeholders about cyber security risk.	The State of Florida agrees that cyber security risk must be shared. The State suggests including language regarding the synergistic benefits of utilizing existing information-sharing infrastructure, such as the Fusion Centers operating across the Nation.		
11	13	2.4 2.e User Configuration and Visibility of Security – Provide an opportunity for the user to check if the security features are in operation	The State of Florida agrees that the Offeror should provide an indication of security features. The State suggests that FirstNet include language regarding current notification best practices, such as a visible icon. This may help reduce confusion and increase efficiency since a user will not have to search for an indication of security.		

12	14	2.4 4. Federal Bureau of Investigation's (FBI) CJIS Security Policy, which includes all those that support the FBI and Department of Justice [CJISD-ITS-DOC-08140-5.0].	The State of Florida maintains that the network shall be CIJS and HIPPA compliant. The State notes, however, that the network must not be precluded from other functions due to stringent and bureaucratic requirements.		
13	15	2.5 6.d. Runs large-scale scheduled cyber security exercises and targeted local cyber security exercises as needed.	The State of Florida requests FirstNet to update the language of this clause from "as needed" to a continuous, predetermined and agreed upon timetable.		
14	15	2.5 7.a, c Engineering a Resilient Network. This requires balancing single-points-of-failure and economics. In short, it is about understanding and managing risk. FirstNet's network architecture, which will ensure that single points of failure are reduced as low as economically reasonable.	The State of Florida understands that there will be a finite amount of economic resources. The network must meet the intent of the Middle Class Tax Relief and Job Creation Act of 2012, though. Therefore, the State requests clarification of the definition of "economically reasonable". Additionally, the State believes it is the intent of the Act, through required State consultation, that the State aid in the definition of "economically reasonable".		
15	16	2.7 1.i-k. i. Provide an after action report for any incident that occurs due to inadvertent actions by authorized operations and maintenance personnel in a format agreed upon by the contractor and FirstNet. j. All security incidents are recorded or logged into an electronic format (to be determined). These logs will provide the information for reporting purposes. k. All security incidents are reported based on incident severity, as directed in standard operating procedures that will be developed jointly between the contractor and FirstNet.	The State of Florida requests that FirstNet include language regarding information sharing between the Offeror, FirstNet, *and* the States in all of the clauses listed. The State also requests a defined timeframe for incidents to be disclosed to the State, as well as the protocol to be enacted for conveyance of the disclosure.		
16	16, 17	2.7 2.b, e, h. b. 24/7/365 cyber security monitoring of core infrastructure e. Establishment of the baseline network activity and utilization to use as a reference	The State of Florida believes it is imperative for Public Safety users to be knowledgeable of any network intrusions in order to maintain the highest level of cyber security. Therefore, the State requests that language be included regarding direct information sharing to each State. The State also		

		h. Information Sharing and Collaboration that integrates and disseminates information throughout the critical infrastructure partnership network. Processing and posting Suspicious Activity Reports. All incidents must be immediately reported, whether suspected or confirmed, involving potential risks to the confidentiality, integrity, or availability of FirstNet information or to the function of NPSBN systems operated on behalf of FirstNet. Upon becoming aware of any unlawful access to any FirstNet data or information stored on the contractor's equipment or in contractor's facilities, or unauthorized access to such facilities or equipment resulting in loss, disclosure, or alteration of any FirstNet data or information (a "Security Incident"), the contractor will notify the contracting officer immediately.	requests a defined timeframe for incidents to be disclosed to the State, as well as the protocol to be enacted for conveyance of the disclosure.		
17	18	2.9 4. Independent Applications/Services Testing – All applications that are distributed by the core network or exchange data with the core network will need a formal testing, validation, and authentication process prior to distribution to provide reasonable assurance of their respective security posture.	The State of Florida agrees that testing, validation, and authentication are necessary to maintain data confidentiality, integrity, and availability. The State maintains that consistent to the Act, through required State consultation, that the State aid in the definition of "reasonable assurance" of security.		
18	18	2.10 1.a. If this is not practical, then alternative methods, such as VPN, are critical.	The State of Florida requests a definition of "practical". Additionally, if an "out of band network" is not "reasonable", then the Offeror shall supply a best practice solution to Public Safety users, as agreed upon in the State Plan.		
19	19	2.10 5a. Security Information and Event Management – SIEM is a tool focused on the security aspects of log management, which involves collecting, monitoring, and analyzing security-related data from computer logs. Security–related data includes log data generated from numerous sources, including antivirus software, intrusion detection systems, file systems, firewalls, routers	The State of Florida agrees that a SIEM tool will be necessary to maintain security. While the State understands that the information gathered may be too technical for a majority of end users, the Offeror could create a high-level mapping tool which shows, in colors (such as green, yellow, and red), the status of the network. Additionally, the State requests FirstNet to update the language of		

		and switches, and servers. The SIEM is responsible for the aggregation and normalization of security-related data and allows for analysis on a large number of logs in an efficient manner.	this clause to include information sharing directly to States through Fusion Centers, Network Operation Centers, or some other existing information sharing infrastructure.		
20	20	2.11 1. However, because the FirstNet wireless network will be disparately deployed across the nation, this can become cost-prohibitive rapidly.	The State of Florida believes this sentence is inappropriate and does not meet the intent of the Act. The State understands that each State may have their own set of potential risks and threats. This does not mean that hardening should not be provided to every State, however. The State also understands that physical security and hardening will be too expensive to provide to every cell site. Therefore, the State maintains that FirstNet, acting through the required State consultation, provide specific and agreed upon hardening requirements for the State Plan.		
21	20	2.12 4-5. 4. Retention of any data will be in accordance with agency record retention policy as specified by the respective data owner. Upon expiration of the retention period, data will be destroyed or otherwise disposed per agency policy. 5. Data in the NPSBN will not be releasable to any external parties without compliance with applicable law.	The State of Florida agrees that local data retention policies, along with Federal policies, must be followed in this network. The State requests language regarding the physical destruction and/or hard drive wiping requirements to be added to this appendix.		